Congressional Research Service
Informing the legislative debate since 1914

Digital Searches and Seizures: Overview of Proposed Amendments to Rule 41 of the Rules of Criminal Procedure

Richard M. Thompson II
Legislative Attorney

June 29, 2016

Congressional Research Service
7-5700
www.crs.gov
R44547

CRS REPORT
Prepared for Members and
Committees of Congress

Contents

Appendixes

Contacts

With the Rules Enabling Act,[1] Congress granted to the Supreme Court the authority to write federal rules of procedure, including the rules of criminal procedure. After several years of evaluation by the Judicial Conference, the policy-making arm of the federal judiciary,[2] on April 28, 2016, the Supreme Court transmitted to Congress proposed changes to Rule 41 of the Federal Rules of Criminal Procedure.[3] These proposed changes would amend the federal search and seizure rules to permit the government to remotely access electronic devices although the location of the device may be unknown. This issue has become more pressing in recent years with an increasing number of users anonymizing their communications, hindering the government's ability to pinpoint the location of the target, and thus making it difficult to discern the appropriate federal court to apply for a search warrant.[4]

In recent years, a tension has arisen between Rule 41 as currently drafted and the Department of Justice's (DOJ's) desired use of the rule for digital searches. This issue arose recently in a 2012 magistrate judge's ruling from the Southern District of Texas, in which the court denied DOJ's application to conduct remote searches of a computer believed to have been part of a fraudulent scheme, because the government could not establish the location of the target, thereby placing it outside the scope of Rule 41 and in violation of the Fourth Amendment particularity requirement.[5]

There have been at least two lines of argument against the proposed rule change, one based on the substance of the proposed amendment and the other grounded in the process by which the rule is being changed. The substantive arguments pertain to the actual substance of the rule and include for example, an argument that the new rule would breach the particularity requirement of the Fourth Amendment.[6] The procedural arguments pertain to how this potential authorization should be made law: through the rulemaking process by the courts or through enacted legislation by Congress.[7] While federal law enforcement has been supportive of the proposed change,[8] some advocacy groups have argued that the proposed rule change "would have significant legal and technical implications" and thus "merit[s] open consideration by Congress, rather than a rulemaking proceeding of the Judicial Conference."[9]

---

[1] *See* 28 U.S.C. §§ 2071-77.

[2] *See* 28 U.S.C. § 331 ("The Conference shall also carry on a continuous study of the operation and effect of the general rules of practice and procedure now or hereafter in use as prescribed by the Supreme Court for the other courts of the United States pursuant to law. Such changes in and additions to those rules as the Conference may deem desirable to promote simplicity in procedure, fairness in administration, the just determination of litigation, and the elimination of unjustifiable expense and delay shall be recommended by the Conference from time to time to the Supreme Court for its consideration and adoption, modification or rejection, in accordance with law.").

[3] *See* Rules Package in Support of Amendments to Federal Rules of Procedure 201 (Apr. 28, 2016), *available at* http://www.uscourts.gov/file/document/2016-04-28-final-package-congress [hereinafter Rules Package].

[4] *See* DOJ Memorandum to Members of Criminal Rules Advisory Committee (March 17, 2014), *in* Advisory Committee on Criminal Rules, Agenda Book April 7-8, 2014 (April 2014), *available at* http://www.uscourts.gov/rules-policies/archives/agenda-books/advisory-committee-rules-criminal-procedure-april-2014 [hereinafter Agenda Book, April 7-8].

[5] *In re* Warrant to Search a Target Computer at Premises Unknown, 958 F. Supp. 2d 753, 759 (S.D. Tex. 2013).

[6] *See* Particularity of Search, *infra* p. 4.

[7] *See* Process Concerns, *infra* p. 7.

[8] *See* Rationale for Amendment, *supra* pp. 4-5.

[9] Written Statement, Center for Democracy and Technology, Before the Judicial Conference Advisory Committee on Rules (Oct. 24, 2014), *available at* https://www.regulations.gov/document?D=USC-RULES-CR-2014-0004-0009 [hereinafter CDT, Written Statement].

This report provides a brief overview of the proposed amendment to Rule 41. First, it provides a background on the origin of, and rationale underlying, the proposed amendment and a description of the rule as currently written. Second, it reviews the potential changes made by the proposed amendment and will survey various concerns commenters have raised with the proposal. Lastly, this report addresses efforts being made in Congress to alter, delay, or stop this rule change.

Background on Amendment to Rule 41

Current Version of Rule 41

Rule 41 of the Rules of Criminal Procedure governs the procedures for obtaining a search warrant in federal court.[10] Among other elements, it requires a government official to demonstrate probable cause that evidence of a crime will be found in the place to be searched.[11] As to the question of venue—that is, which is the appropriate federal district court to seek a search warrant—Rule 41 provides that a search warrant may be issued by "a magistrate judge with authority in the district."[12] Rule 41 permits the issuance of *extraterritorial* warrants (warrants to be served outside of that judge's jurisdiction) in four limited instances: (1) the property is within the jurisdiction but may be moved out of the jurisdiction before the warrant is executed; (2) the property is part of an investigation of domestic or international terrorism; (3) tracking devices are used which can be monitored outside the jurisdiction if installed within the jurisdiction; or (4) the property is located in a U.S. territory or U.S. diplomatic or consular mission.[13] However, based on the text of the rule, none of these exceptions appear to permit searches where the location of the target is unknown, such that it is not clear in which jurisdiction to request a warrant.

In a 2012 magistrate judge's ruling from the Southern District of Texas, the government requested a search warrant to remotely search an unknown computer in an unknown location that was believed to have been used to perpetrate a fraudulent scheme.[14] The government wanted access to, among other things, IP addresses used; records of Internet activity, including browsing history and search terms used; and photographs taken using the computer's built in camera.[15] Magistrate Judge Stephen Smith rejected the government's application on two grounds. First, Judge Smith found that the government's application did not meet one of the territorial limitations found in the Rule.[16] Second, he found that the application failed to meet the particularity requirement contained in the Fourth Amendment, which requires that "no warrants shall issue, but upon probable cause, supported by Oath or affirmation, and *particularly describing the place to be searched, and the persons or things to be seized*,"[17] as the government failed to explain how the target device was to be found.[18] Further, Judge Smith noted the risk of targeting innocent computers when the location of the target is unknown.[19]

[10] FED. R. CRIM. P. 41.

[11] *Id.* at (d)(1).

[12] *Id.* at (b)(1).

[13] FED. R. CRIM. P. 41(b)(2-5).

[14] *In re* Warrant to Search a Target Computer at Premises Unknown, 958 F. Supp. 2d 753, 755 (S.D. Tex. 2013).

[15] *Id.* at 755-56.

[16] *Id.* at 758.

[17] U.S. CONST. amend. IV (emphasis added).

[18] *In re Warrant*. 958 F. Supp. 2d at 759.

[19] *Id.*

Amendment Process

Prompted partially by the ruling from the Southern District of Texas, the proposal to amend Rule 41 was first brought to the attention of the Judicial Conference in a September 2013 memorandum from DOJ, which highlighted two "increasingly common situations" faced by investigators that warranted a change in the rules.[20] The first is where the warrant sufficiently describes the device to be searched, but law enforcement officials do not know the location of the target device. The second is where the investigation requires officials to engage in surveillance of numerous computers in multiple jurisdictions. The proposed rule change was published for public comment in August 2014, in which DOJ, privacy advocates, computer experts, and members of the general public offered various arguments for and against the proposed rule change.[21] On April 28, 2016, the Supreme Court transmitted the proposed rule change to Congress. Pursuant to the Rules Enabling Act, unless Congress responds via enacted legislation, the proposed rule will take effect on December 1, 2016.[22]

Proposed Amendment

The proposed amendment was designed to address two issues: (1) access to a device at an unknown location; and (2) access to multiple computers in multiple districts. Each will be addressed in turn.

Searches of Devices with Unknown Locations

The first rationale for amending Rule 41 applies to situations when the government is able to describe the computer to be searched, but does not know the location of the computer. DOJ asserted, and the Judicial Conference accepted, that the government faces this situation more regularly because persons who commit crimes on the Internet are using anonymizing technologies with greater frequency.[23] Through the use of proxy servers, criminals are able to mask their IP addresses such that the recipient only knows the IP address of the proxy and not the originator's IP address.[24]

To permit extraterritorial searches, Rule 41 would be amended to read as follows:

> a magistrate judge with authority in any district where activities related to a crime may have occurred has authority to issue a warrant to use remote access to search electronic storage media and to seize or copy electronically stored information located within or outside that district if ... the district where the media or information is located has been concealed through technological means[.][25]

[20] Memo, Department of Justice to Advisory Committee on Criminal Rules 2 (Sept. 18, 2013), *in* Agenda Book, April 7-8, 2014, *supra* note 4, at 172.

[21] *See* Docket Folder, Proposed Amendments to the Federal Rules of Criminal Procedure (last visited June 29, 2016), *available at* https://www.regulations.gov/docket?D=USC-RULES-CR-2014-0004

[22] 28 U.S.C. § 2074.

[23] Advisory Committee on Criminal Rules, Agenda Book, Meeting of March 16-17, 2016, at 88 (2016), *available at* http://www.uscourts.gov/rules-policies/archives/agenda-books/advisory-committee-rules-criminal-procedure-may-2015.

[24] *Id.*

[25] *See* Rules Package, *supra* note 3, at 222.

Multi-device, Multi-district Searches

The second rationale for amending Rule 41 applies to situations where the government needs to search multiple computers in numerous districts as part of a large-scale investigation of computer crimes.[26] Under the current rule, there are limited mechanisms for seeking a warrant outside of the judicial district in which a computer is located, but none cover the type of authorization DOJ seeks here.[27] In its submission to the Judicial Conference, DOJ argued that effective investigation of large-scale online attacks, such as botnets—an "interconnected network of computers infected with malware without the user's knowledge and controlled by cybercriminals"[28]—requires a change to Rule 41 such that government officials can seek authorization in one district court, although the criminal activity may span multiple districts.[29]

As submitted to Congress, the second prong of the proposed rule change reads as follows:

> a magistrate judge with authority in any district where activities related to a crime may have occurred has authority to issue a warrant to use remote access to search electronic storage media and to seize or copy electronically stored information located within or outside that district if ... (B) in an investigation of a violation of 18 U.S.C. § 1030(a)(5), the media are protected computers that have been damaged without authorization and are located in five or more districts.[30]

This change would allow DOJ to remotely access a potentially large number of affected computers, without having to apply for a warrant in each judicial district in which an affected computer is located.

Issues Raised by Proposed Amendment to Rule 41

As part of the review process, the Advisory Committee received comments both supporting and opposing the proposed amendment to Rule 41. The Advisory Committee noted that "the most common theme in the comments opposing the amendment was concern that it relaxed or undercut the protections for personal privacy guaranteed in the Fourth Amendment."[31] Objectors made other arguments against the proposal including that it might engender forum shopping. This section will briefly explore these and other concerns raised by public comments.

Rationale for Amendment

Several commenters have proffered various arguments in support of the proposed rule change. First, and perhaps most obviously, is the fact that DOJ has been prevented in at least one reported ruling from remotely searching a target's computer when it could not state the location of the target.[32] More generally, DOJ has argued that criminals are using anonymizing techniques more frequently, so that DOJ is able to identify the computer but not the location of the target. In this

[26] *Id.* at 89.

[27] FED. R. CRIM. P. 41(b)(2)-(5).

[28] *See* What is a Botnet Attack? – Definition, Kaspersky Lab (last visited June 29, 2016), https://usa.kaspersky.com/internet-security-center/threats/botnet-attacks#.V3QTpfkrJbU.

[29] See Agenda Book, April 7-8, 2014, *supra* note 4, at 156.

[30] *See* Rules Package, *supra* note 3, at 223. Federal law outlaws the transmission of a program or command with the intent to damage a computer system. *See* 18 U.S.C. § 1030(a)(5).

[31] Memorandum from Reporters to Advisory Committee on Rules, Rule 41 (Feb. 25, 2015), *in* Advisory Committee on Criminal Rules, Agenda Book, Meeting of Mar. 16-17, 2015 [hereinafter Agenda Book, March 2015].

[32] *See* Current Version of the Rule, *supra* p. 2.

vein, DOJ has argued that "there is a substantial interest in catching and prosecuting criminals who use anonymizing technologies, but locating them can be impossible for law enforcement absent the ability to conduct a remote search of the criminal's computer."[33] As to the second proposed change—investigation of botnet-like schemes that involve many computers in many districts—the National Association of Assistant United States Attorneys argued that coordinating many requests and review by many magistrate judges "not only wastes judicial and investigative resources, but also may cause delay that impedes investigation."[34]

Particularity of Search

Opponents of the proposed amendment to Rule 41 have argued that it would violate the particularity requirement of the Fourth Amendment. Again, the Fourth Amendment requires that no warrant shall issue unless it "*particularly describe[s] the place to be searched, and the persons or things to be seized*."[35] These observers cite to the Southern District of Texas ruling, which held that an extraterritorial warrant would violate the Fourth Amendment particularity requirement because it failed to state a location for the computer.[36]

In response to this concern, the Advisory Committee included a Committee Note to Rule 41, providing the following explanation about how the Fourth Amendment should apply to the proposed amendment:

> The amendment does not address constitutional questions, such as the specificity of description that the Fourth Amendment may require in a warrant for remotely searching electronic storage media or seizing or copying electronically stored information, leaving the application of this and other constitutional standards to ongoing case law development.[37]

However, some privacy advocates believe that this proviso will be largely ineffective. For example, the Center for Democracy and Technology (CDT) noted that while "the Committee does not seek to address such questions in this rulemaking, the proposed modification to Rule 41 nonetheless does have direct bearing on these very questions since it specifically contemplates the issuance of warrants for computers in concealed locations."[38]

Surreptitious Entry, Destructive Searches

At least one observer has argued that the proposed amendment cannot meet the more demanding Fourth Amendment standard required for covert-entry remote access searches,[39] which generally requires that the government has some "reasonable necessity" for conducting the surreptitious search and that notice be given a reasonable time after the search is conducted.[40] Others have argued that the use of "malware and zero-day exploits is more invasive than other forms of

[33] *See* Agenda Book, April 7-8, *supra* note 4, at 172.

[34] *See* Written Comment on Rule 41, National Association of Assistant United States Attorneys (Feb. 4, 2015), *available at* https://www.regulations.gov/document?D=USC-RULES-CR-2014-0004-0027.

[35] U.S. CONST. amend. IV (emphasis added).

[36] CDT, Written Statement, *supra* note 9.

[37] Rules Package, *supra* note 3.

[38] CDT, Written Statement, *supra* note 9.

[39] Electronic Privacy Information Center, Statement on Proposed Amendments to Rule 41 of the Federal Rules of Criminal Procedure (Nov. 5, 2014), *available at* https://www.regulations.gov/document?D=USC-RULES-CR-2014-0004-0010.

[40] *See* United States v. Villegas, 899 F.2d 1324, 1337 (2d Cir. 1990).

permissible searches because the consequences and collateral damage associated with their use are inherently unpredictable and often irreversible."[41] Like with the particularity arguments, discussed earlier, the Judicial Conference responded to these comments by highlighting the Committee Note, which asserts that the rule "does not foreclose or prejudge these constitutional issues," but rather "leaves them to be resolved on a case-by-case basis."[42]

Notice

Several commenters challenged the sufficiency of the notice requirements provided under the proposed rule. The American Civil Liberties Union (ACLU), for instance, argued that the notice requirements were lessened under the proposed amendment as they did not require that the officer "must" provide a copy of the warrant—as is required currently under Rule 41(f)(1)(C)—but instead would require only that the officer "make reasonable efforts to serve a copy of the warrant and receipt" and ensure service is "reasonably calculated to reach that person."[43] The ACLU argued that providing notice will be difficult in many common situations, such as a target who signs onto a wireless network at a coffee shop or library.[44] In response, the Advisory Committee described the proposed notice requirements as "intended to be parallel, to the degree possible, with the requirement for physical searches."[45] Providing notice in the case of physical searches is not always possible, the Committee noted, and the rule as currently written does not require actual notice, but rather that notice be given "to the person from whom, or from whose premises, the property was taken, or leave a copy of the warrant and receipt at the place where the officer took the property."[46]

Additionally, the ACLU argued that the government should have to provide notice to both the owner of a computer *and* others who may have used and stored information on that device, not one *or* the other as is currently proposed in the rule.[47] The Judicial Conference rejected this suggestion, claiming that if the government executes a warrant for a business and seizes records of individual customers, providing notice to each customer would be too burdensome on the government, and is not required under current law.[48]

Finally, several commenters argued that government officials could delay giving notice, as the proposed notice requirement only requires that the government make "reasonable efforts" to provide notice, but does not require that it be given promptly.[49] Answering these comments, the Committee noted that Rule 41(f)(3) permits delayed notice if permitted by statute. The Committee added a Committee Note stating that "Rule 41(f)(3) allows delayed notice *only* 'if the delay is authorized by statute.'"[50]

---

[41] *See* Amer. Civil Liberties Union, Second Comment on the Proposed Amendment to Rule 41 Concerning "Remote Access" Searches of Electronic Storage Media 23-24 (Oct. 31, 2014), *available at* https://www.regulations.gov/document?D=USC-RULES-CR-2014-0004-0013ACLU [hereinafter ACLU, Second Comment].

[42] *See* Agenda Book, March 2015, *supra* note 31, at 92.

[43] ACLU Second Comment, *supra* note 41, at 23-24; Final Rules Package, *supra* note 2, at 224.

[44] ACLU Second Comment, *supra* note 41.

[45] Agenda Book, March 2015, *supra* note 31, at 93.

[46] FED. R. CRIM. P. 41(f)(1)(C).

[47] ACLU, Second Comment, *supra* note 41, at 24.

[48] Agenda Book, March 2015, *supra* note 31, at 93-94.

[49] *See* ACLU, Second Comment, *supra* note 41, at 24-25; EPIC, Written Statement, *supra* note 37.

[50] Rules Package, *supra* note 3 (emphasis added).

Impediments to Judicial Review

Some commenters also raised concerns that the proposed rule, combined with existing judicial doctrines, could hinder judicial review in various ways, including:

- *Ex parte proceedings and lack of technical sophistication in the judiciary.* Warrant proceedings are largely resolved *ex parte*—that is, only the government's attorney is present to offer arguments to the magistrate judge. Some have argued that the nature of these one-sided proceedings would hinder effective judicial review, especially when difficult technological questions are involved.[51]
- *Good Faith.* Under the good faith exception to the exclusionary rule of the Fourth Amendment, unlawfully obtained evidence can still be admissible in a criminal trial if the evidence was "obtained in objectively reasonable reliance on a subsequently invalidated search warrant."[52] Some have argued that, because courts have the authority to resolve the good faith question before the substantive Fourth Amendment question,[53] the constitutional merits could largely go unresolved.[54]
- *Qualified Immunity*. Qualified immunity operates in a similar manner in the civil context as good faith does in the criminal context: it "protects government officials from liability for civil damages insofar as their conduct does not violate clearly established statutory or constitutional rights of which a reasonable person would have known."[55] Again, courts are permitted to resolve this procedural question before moving to the merits of the plaintiff's claim.[56] Commenters have posited that qualified immunity, like good faith, could preclude judicial review of the constitutionality of these largely untested search and seizure techniques.[57]

Forum Shopping

Some have argued that permitting remote searches under Rule 41 in any district in which an element of the crime occurred raises significant concerns of forum shopping. That is, they argue that when the government has multiple options of jurisdictions in which to file a warrant application, it will more often than not choose the more government-friendly judge.[58]

Process Concerns

In addition to comments concerning the changes to Rule 41 itself, many observers have challenged the method in which the rule is being changed. Some have argued that as sensitive a

[51] *See, e.g.*, ACLU, Second Comment, *supra* note 41, at 25-26.

[52] *See* United States v. Leon, 468 U.S. 897, 922 (1984).

[53] *See*., *e.g.*, United States v. Clay, 646 F.3d 1124, 1128 (8th Cir. 2011).

[54] *See* ACLU, Second Comment, *supra* note 41, at 26 ("[E]ven in cases where a remote access warrant fails the particularity, probable cause, or reasonableness requirements of the Fourth Amendment, courts will generally avoid ruling on the issue.").

[55] Harlow v. Fitzgerald, 457 U.S. 800, 818 (1982).

[56] *See* Pearson v. Callahan, 555 U.S. 223, 236 (2009).

[57] *See* ACLU, Second Comment, *supra* note 41, at 26-27.

[58] CDT, Written Statement, *supra* note 9, at 5.

topic as remote hacking should undergo a more thorough vetting via the formal congressional lawmaking process rather than through the rulemaking process of a federal agency.[59] As argued by the Center for Democracy & Technology:

> The proposed changes to FRCrmP Rule 41 are not a Congressional amendment, nor do they implement a direct expansion of extraterritorial jurisdiction codified in statute. Congress has not authorized extraterritorial or multi-district searches for computers with concealed locations or during investigations under 18 U.S.C. § 1030(a)(5), as the proposed modification to Rule 41 contemplates. The proposed modification attempts to expand magistrates' Rule 41 authority in a manner that has historically been accomplished by Congressional action. The proposed modification should be handled through Congress rather than judicial rulemaking.[60]

Congressional Action

Upon transmittal of the proposed amendment to Rule 41, Senator Ron Wyden introduced the Stopping Mass Hacking Act (S. 2952, H.R. 5321) to reject this rule change. It would provide as follows:

> The proposed amendments to rule 41 of the Federal Rules of Criminal Procedure, which are set forth in the order entered by the Supreme Court of the United States on April 28, 2016, shall not take effect.[61]

Again, if Congress does not act, the proposed amendment will take legal effect on December 1, 2016.[62]

[59] *Id.*

[60] *Id.*

[61] S. 2952, 114th Cong. (2016); H.R. 5321, 114th Cong. (2016).

[62] *See* 28 U.S.C. § 2074.

Appendix. Text of Proposed Amendment to Rule 41

The following language is the final proposed amendment transmitted from the Supreme Court to Congress:

> Rule 41. Search and Seizure.
>
> …
>
> (b) ~~Authority to Issue a Warrant~~. Venue for a Warrant Application.
>
> At the request of a federal law enforcement officer or an attorney for the government:
>
> …
>
> (6) a magistrate judge with authority in any district where activities related to a crime may have occurred has authority to issue a warrant to use remote access to search electronic storage media and to seize or copy electronically stored information located within or outside that district if: (A) the district where the media or information is located has been concealed through technological means; or
>
> (B) in an investigation of a violation of 19 18 U.S.C. § 1030(a)(5), the media are protected computers that have been damaged without authorization and are located in five or more districts.
>
> (f) Executing and Returning the Warrant.
>
> (1) Warrant to Search for and Seize a Person or Property.
>
> …
>
> (C) Receipt. The officer executing the warrant must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken or leave a copy of the warrant and receipt at the place where the officer took the property. For a warrant to use remote access to search electronic storage media and seize or copy electronically stored information, the officer must make reasonable efforts to serve a copy of the warrant and receipt on the person whose property was searched or who possessed the information that was seized or copied. Service may be accomplished by any means, including electronic means, reasonably calculated to reach that person.[63]

Author Contact Information

Richard M. Thompson II
Legislative Attorney
rthompson@crs.loc.gov, 7-8449

[63] Rules Package, *supra* note 2.